CVCI
CHAMBRE VAUDOISE
DU COMMERCE ET
DE L'INDUSTRIE

LES ENTREPRISES VAUDOISES FACE AUX ENJEUX DE LA CYBERSÉCURITÉ

LE PARTENAIRE DES ENTREPRISES

TABLE DES MATIÈRES

4 LA CYBERSÉCURITÉ, DÉFI MAJEUR POUR LES ENTREPRISES VAUDOISES

6 LA STRUCTURE DE L'ÉCHANTILLON

7 LA CONNAISSANCE DE LA THÉMATIQUE

8 LE NIVEAU D'INFORMATION

11 LA SENSIBILITÉ AUX CYBER-RISQUES

14 LES CYBERATTAQUES SUBIES

18 LES MESURES DE PROTECTION

22 LA PLACE DE LA FORMATION

24 LA GESTION DES DONNÉES PERSONNELLES

26 LES CLÉS DE LA SÉCURITÉ NUMÉRIQUE

Étude réalisée sur la base du sondage effectué par la société M.I.S Trend à Lausanne, sur mandat de la CVCI

Responsable de la communication : Fanny Oberson Gross, fanny.oberson@cvci.ch
Texte : Jean-François Krähenbühl, chargé de communication, jfk@cvci.ch

Conception et réalisation : DO! L'agence SA

Septembre 2018

LA CYBERSÉCURITÉ, DÉFI MAJEUR POUR LES ENTREPRISES VAUDOISES

LES PME DANS L'ŒIL DU CYBERESPACE

La digitalisation de l'économie connaît un développement spectaculaire, comme le soulignait la Chambre vaudoise du commerce et de l'industrie (CVCI) dans son étude « Les entreprises vaudoises et la transition numérique », publiée au début de l'an dernier. Même s'il ne concerne pas tous les secteurs économiques dans la même mesure, le phénomène prend de l'ampleur avec, pour corollaire, un accroissement significatif des risques de cyberattaques. Celles-ci ne constituent rien d'autre qu'un prolongement de la criminalité du monde physique dans un environnement dématérialisé, car le vol, l'extorsion, l'escroquerie et bien d'autres délits sont hélas transposables dans l'espace virtuel.

Qu'il s'agisse d'une cyberattaque massive comme le logiciel malveillant WannyCry, qui a touché plus de 300 000 ordinateurs dans plus de 150 pays en mai 2017, ou d'une attaque ciblée, les actes de piratage informatique peuvent engendrer des dommages considérables pour une entreprise, telles des pertes de données, des perturbations de services, des interruptions d'activités, voire, dans le pire des scénarios, une faillite. Le Code pénal suisse réprime un certain nombre d'infractions liées à l'informatique. Mieux vaut cependant prévenir que guérir, car restaurer des systèmes piratés peut coûter très cher alors que, dans le même temps, il est très difficile de mettre la main sur les auteurs de ces délits, qui sont souvent à l'œuvre depuis des pays étrangers. Dernier exemple marquant en date: le Ministère public de la Confédération a annoncé, en août dernier, qu'il n'était pas parvenu à identifier les auteurs de la cyberattaque perpétrée en 2016 contre le groupe d'aéronautique et de défense suisse Ruag. Et a dû se résoudre à suspendre la procédure pénale en cours…

Une enquête de l'Institut de sondages et d'études de marché gfs-zürich, parue l'hiver dernier, révélait que plus d'un tiers des PME suisses ont été confrontées à des malwares, tels que des virus et des chevaux de Troie. Plus inquiétant encore, l'immense majorité des patrons sondés considéraient comme négligeable le risque d'être touché. Réagissant à ces résultats, un membre de l'Association suisse d'assurances exprimait son inquiétude en ces termes: « Plus de 98 % des entreprises suisses sont des PME; elles constituent la colonne vertébrale de l'économie du pays. Il est donc d'une importance stratégique pour la Suisse que ces entreprises soient mieux protégées contre les cyber-risques. » Cet été, une société vaudoise s'est fait voler les données de quelque 35 000 clients, lesquelles seront sans doute monnayées sur le Darknet, ce réseau superposé lié aux activités illégales comme la cybercriminalité. Un cas parmi bien d'autres, tant il est vrai que les entreprises ne communiquent pas forcément sur le sujet, ne serait-ce que pour des questions d'image.

UNE BASE PARFAITEMENT EXPLOITABLE

Face à cette évolution préoccupante, la CVCI a souhaité dresser un état des lieux à l'échelle vaudoise. Si le phénomène des attaques informatiques est réel et identifié, nous ne disposons que de peu de données statistiques sur son ampleur. Quels sont les impacts des cyber-risques et des cyberattaques sur les entreprises du canton ? Quelle proportion, parmi celles-ci, a déjà fait l'objet d'attaques informatiques ? Quelles en sont les conséquences financières ? Combien investissent-elles pour s'en prémunir ? Et de quelle manière sensibilisent-elles leur personnel ?

Pour prendre la mesure de la problématique, la CVCI a mandaté l'institut de recherches M.I.S Trend, à Lausanne, afin de sonder directement ses membres. L'objectif a consisté à dégager des tendances et à suggérer des pistes d'amélioration dans les domaines où des manques ont été observés, comme la protection des systèmes, la sensibilisation aux cyber-risques et la formation des collaborateurs.

Le questionnaire adressé à nos membres portait sur divers aspects comme

- la connaissance de la thématique,
- le niveau d'information,
- la sensibilité aux cyber-risques,
- les cyberattaques subies,
- les mesures de protection,
- la place de la formation,
- la gestion des données personnelles.

CONSTATS INQUIÉTANTS

Notre étude, dont les résultats chiffrés sont détaillés dans les pages qui suivent, met en évidence un certain nombre de faits qui démontrent la nécessité impérieuse, pour le monde de l'économie, d'intégrer la cybersécurité dans sa réflexion stratégique. Le premier constat est la réalité des menaces de piratage pour les entreprises. Dans le canton, un tiers d'entre elles révèlent avoir été victimes d'au moins une attaque. Cette proportion confirme les chiffres d'études comparables menées ces derniers mois à l'échelle suisse. En réalité, on peut affirmer que 100 % d'entre elles ont été visées, car toutes reçoivent régulièrement des mails avec des adresses d'expéditeur falsifiées (phishing), estime Patrick Zwahlen, spécialiste de la sécurité informatique chez Navixia, à Écublens. Ces envois, qui proviennent d'organisations mafieuses ayant dérobé des listes d'adresses, sont distribués en masse, tous azimuts. Seulement, et fort heureusement, tous les collaborateurs ne cliquent pas sur les pièces qui y sont jointes ou sur les liens menant à des sites malveillants.

Autre élément de l'étude, tout aussi inquiétant: un tiers des entreprises sondées estiment ne pas être concernées par les cyber-risques, notamment en raison de leur petite taille. Cette vision relève de la naïveté: même une PME active dans un marché de niche peut intéresser des criminels de la Toile, car elle génère des profits et crée des brevets qui peuvent susciter des convoitises.

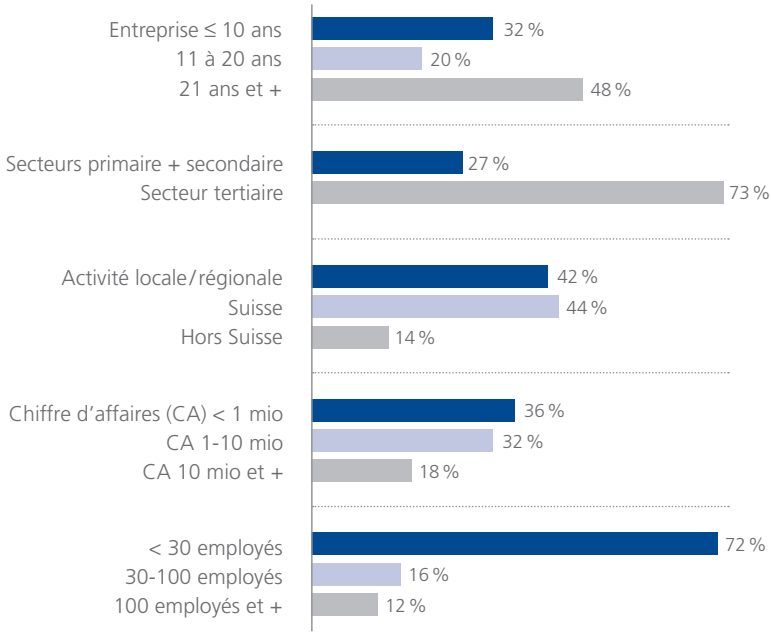
Par ailleurs, il apparaît que la connaissance de la problématique cybersécuritaire est relativement floue. Les entreprises citent spontanément un grand nombre de menaces, mais seules 9 % d'entre elles évoquent celle du phishing, alors que cette méthode constitue, à dire d'experts, la grande majorité des tentatives de piratage. Plus surprenant, les sondés s'informent sur ces problèmes essentiellement via les médias, Internet et le bouche à oreille, négligeant les informations dispensées par les autorités. Ce fait met en lumière un manque à ce niveau. Autre point encore plus sidérant : seuls 32 % des répondants à notre enquête ont mis en place des formations en la matière ou sont sur le point de le faire. C'est là un enjeu crucial dans la lutte contre la cybercriminalité, sur lequel nous reviendrons dans l'analyse de détail.

Avec ses 3200 membres employant quelque 135 000 collaborateurs, la CVCI représente les trois quarts des emplois industriels et, plus globalement, un tiers des emplois privés recensés dans le canton. L'enquête publiée dans cette brochure comporte une marge d'erreur de +/- 4 %, un taux qui permet de tirer des enseignements pertinents.

Seuls 32 % des répondants à notre enquête ont mis en place des formations en la matière ou sont sur le point de le faire.

LA STRUCTURE DE L'ÉCHANTILLON

Base : 490 entreprises membres de la CVCI



Les interviews ont été réalisées du 14 mai au 15 juin 2018 par l'institut de recherche M.I.S Trend, à Lausanne, sur mandat de la CVCI. Un email informatif, adressé à 2734 de nos membres, a annoncé l'étude et mis à disposition un lien sécurisé pour accéder au questionnaire. L'échantillon obtenu représente 490 entreprises membres, soit 18% de l'ensemble, ce qui lui confère une base parfaitement exploitable en termes d'analyse.

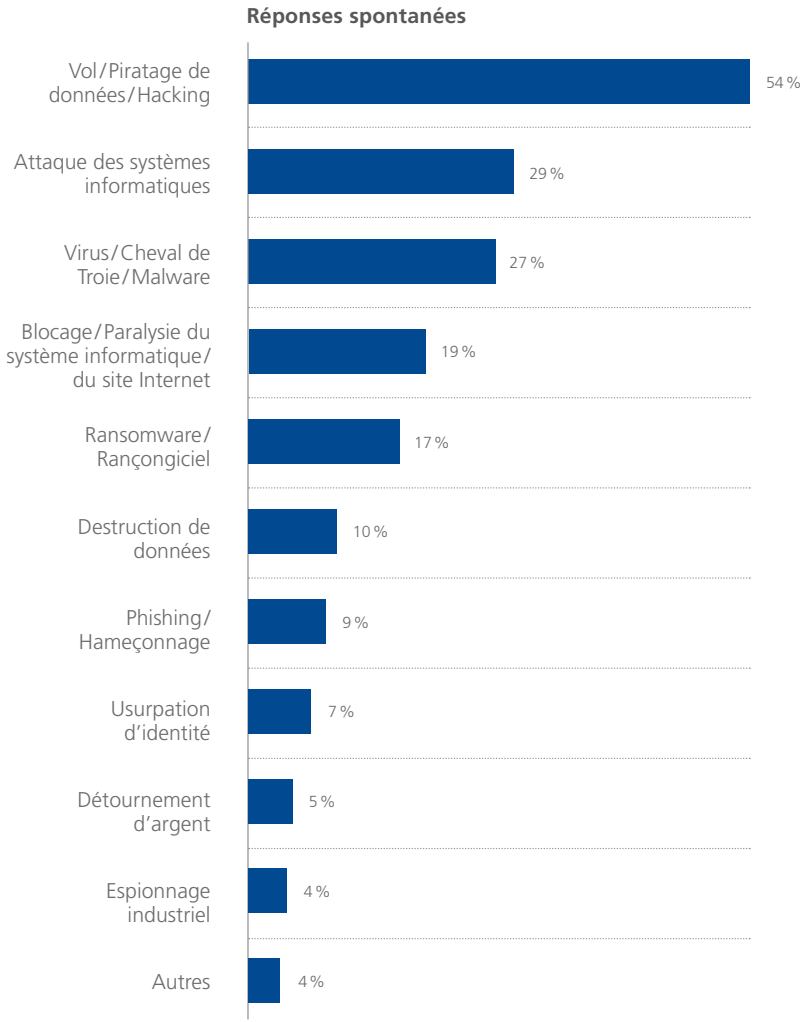
La structure de l'échantillon est comparable, en termes de taille et de secteur d'activité, à l'échantillon obtenu lors des enquêtes conjoncturelles et lors de la dernière étude thématique sur la digitalisation des entreprises, en 2017.

Les résultats globaux n'ont pas été pondérés. La marge d'erreur est de +/- 4,0% sur le total des entreprises ayant répondu à notre coup de sonde.

1. LA CONNAISSANCE DE LA THÉMATIQUE

1.1 Quand on parle de cyber-risques, de cyberattaques, à quels types de menaces pensez-vous ?

Base : 490 entreprises membres de la CVCI

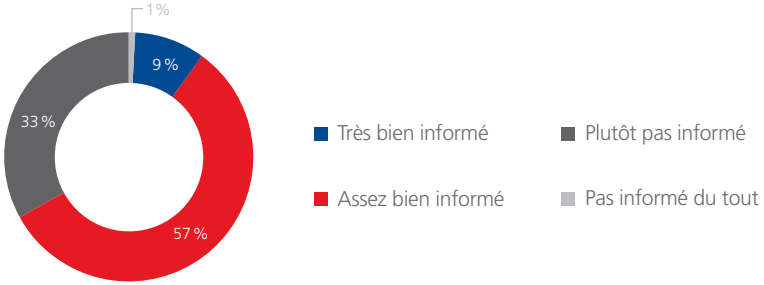


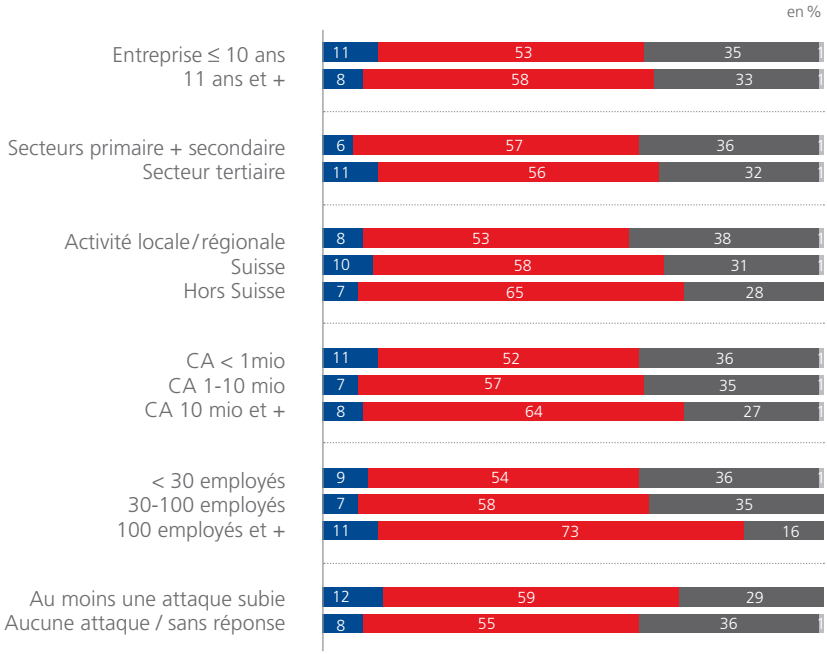
Les sondés mettent le phishing au même niveau que d'autres attaques, mais d'expérience, on sait que ce dernier est le mode opératoire usuel des criminels du Web. Et dans les faits, 100 % des sociétés reçoivent de tels mails frauduleux.

2. LE NIVEAU D'INFORMATION

2.1 D'une manière générale, vous sentez-vous informé sur le thème de la cybersécurité ?

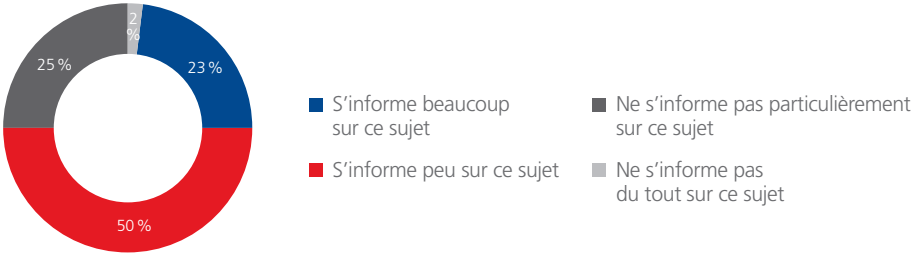
Base : 490 entreprises membres de la CVCI

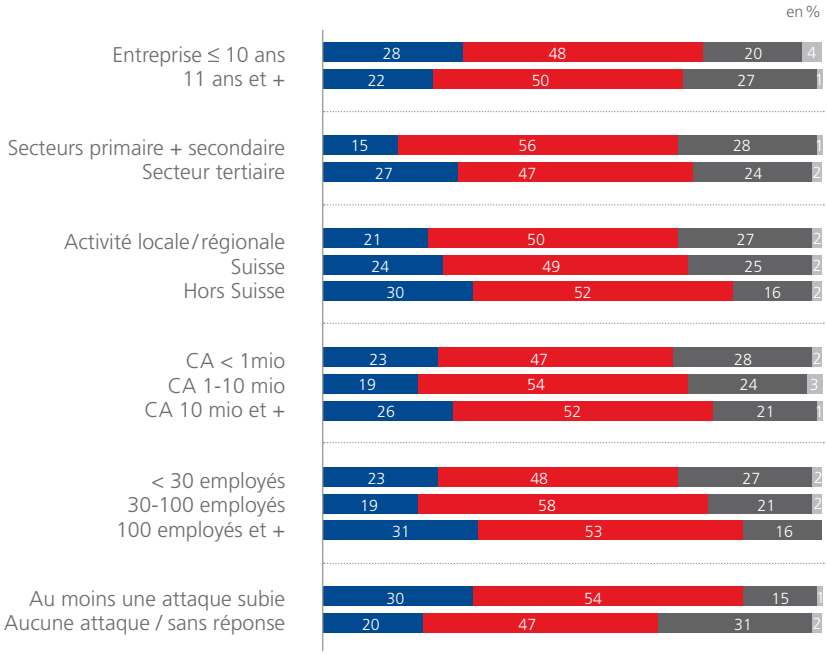




2.2 Est-ce que vous vous informez sur la cybersécurité dans votre entreprise ?

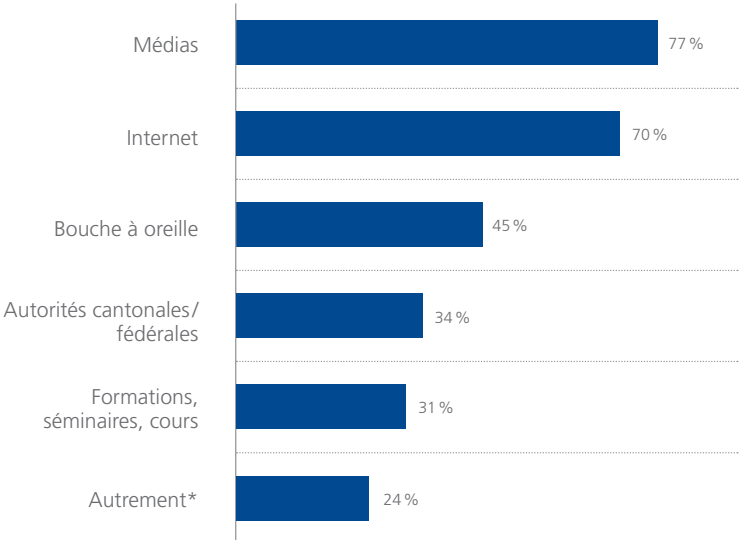
Base : 490 entreprises membres de la CVCI





2.3 Comment vous informez-vous sur le thème de la cybersécurité de manière générale ?

Base : 359 entreprises membres de la CVCI qui s'informent sur la cybersécurité



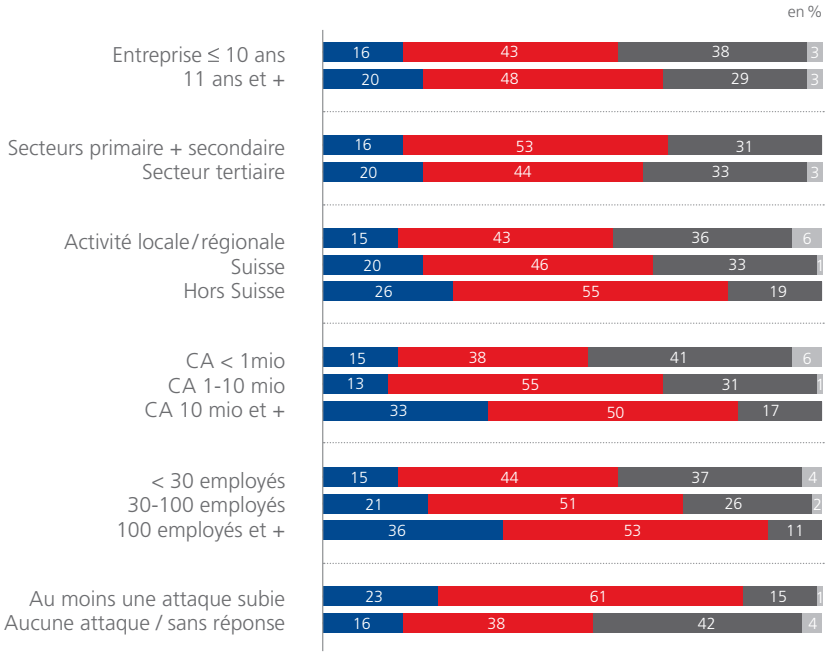
* *Prestataires, consultants (11 %)*
Service IT/informaticiens dans l'entreprise (6 %)
Actifs dans ce domaine (1 %)
Lectures spécialisées (1 %)
Plateforme d'entreprises, échange d'informations (1 %)

Parmi les trois-quarts des sondés qui disent s'informer de manière générale sur le sujet, 77 % le font à travers les médias, 70 % via Internet. « Il peut y avoir un ‹effet *20 minutes*›, souligne l'expert Patrick Zwahlen : un article sur des attaques peut provoquer une prise de conscience. »

3. LA SENSIBILITÉ AUX CYBER-RISQUES

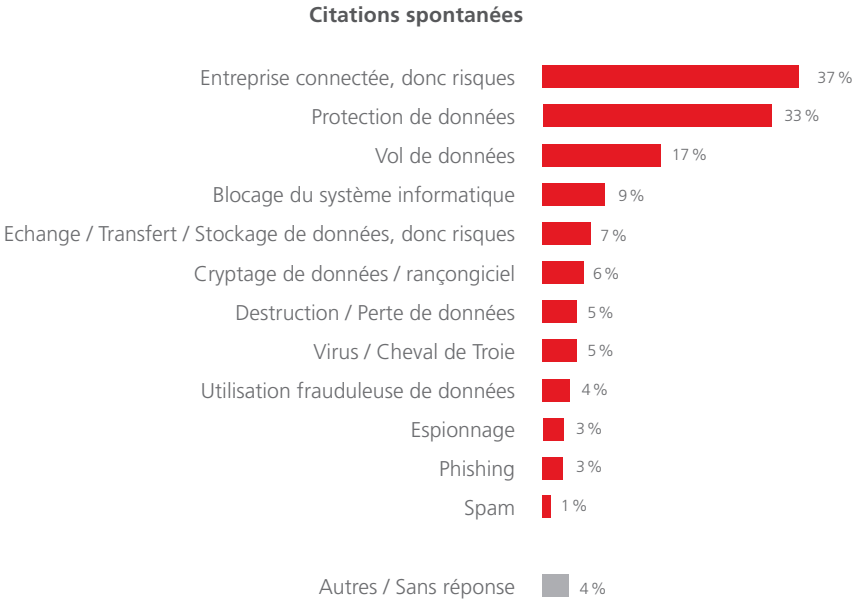
3.1 D'une manière générale, votre entreprise est-elle concernée ou non par les cyber-risques ?

Base : 490 entreprises membres de la CVCI



3.2 Pourriez-vous indiquer en quelques mots en quoi votre entreprise est concernée par les cyber-risques ?

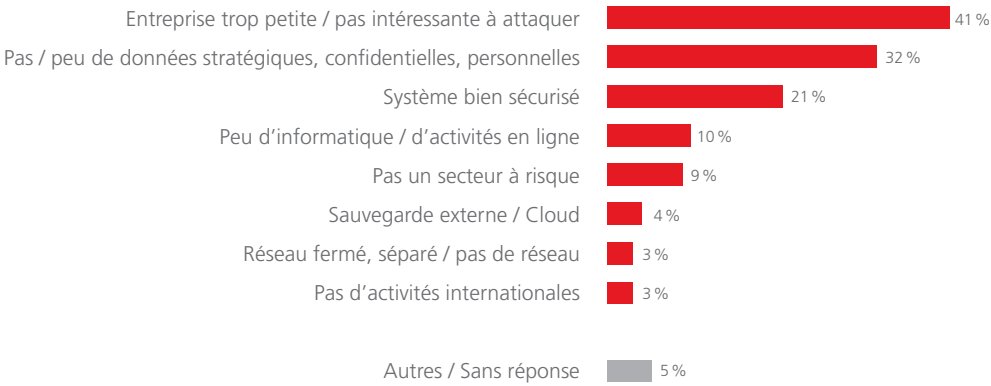
Base : 319 entreprises membres de la CVCI concernées par les cyber-risques



3.3 Pourriez-vous indiquer en quelques mots pourquoi votre entreprise n'est pas (ou plutôt pas) concernée par les cyber-risques ?

Base : 171 entreprises membres de la CVCI pas concernées par les cyber-risques

Citations spontanées

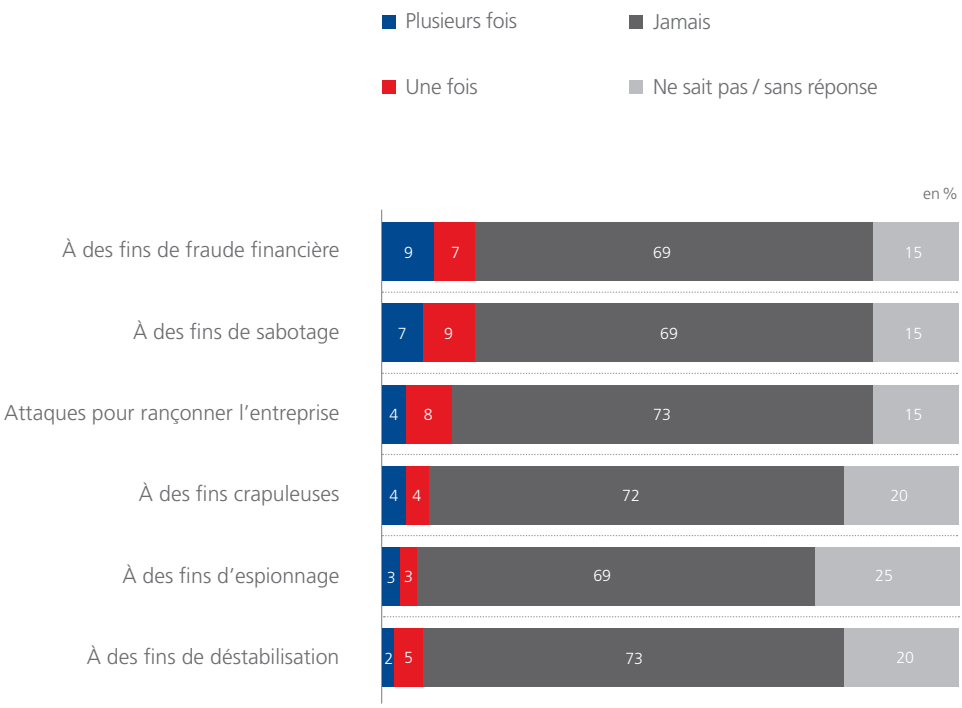


Les experts le disent : le tiers des entreprises qui, selon notre enquête, estiment qu'elles ne sont pas concernées par les cyber-risques, sous-estiment un danger auquel elles seront, tôt ou tard, confrontées.

4. LES CYBERATTAQUES SUBIES

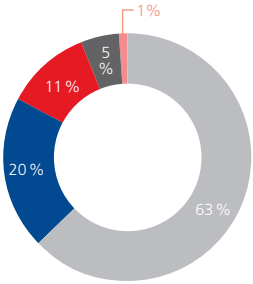
4.1 Votre entreprise a-t-elle déjà été victime des cyberattaques suivantes (via des virus, malwares, chevaux de Troie, phishing…) ?

Base : 490 entreprises membres de la CVCI



4.2 Votre entreprise a-t-elle déjà été victime de cyberattaques ?

Base : 490 entreprises membres de la CVCI



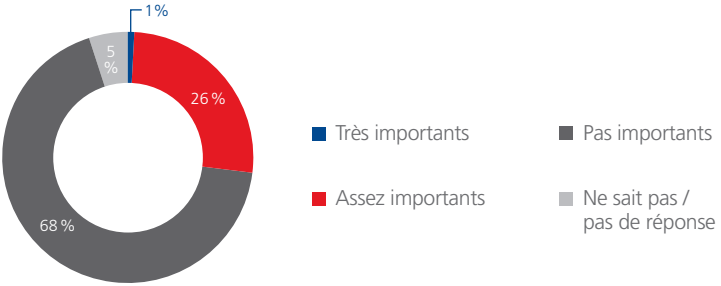
- Aucune
- 1 type d'attaque sur 6
- 2 types d'attaques sur 6
- 3-4 types d'attaques sur 6
- 5-6 types d'attaques sur 6

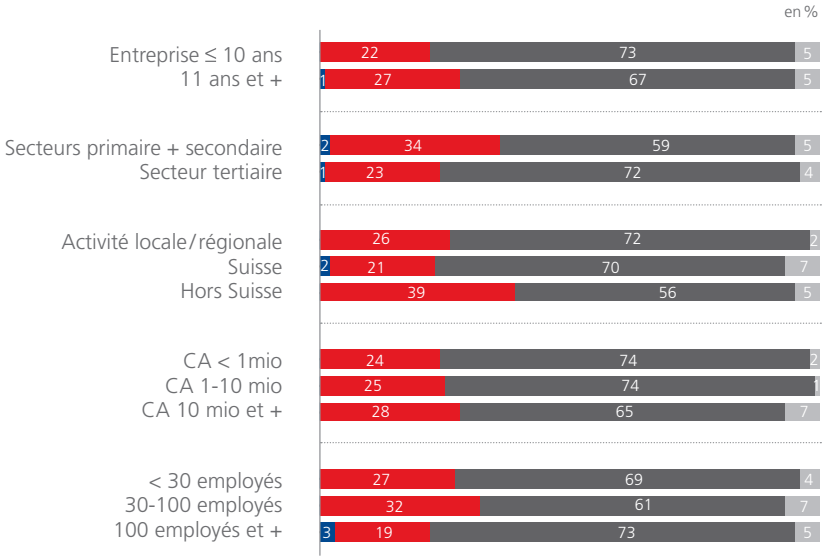
en %

Entreprise ≤ 10 ans	76	14	6	3	1	
11 ans et +	56	23	13	7	1	
Secteurs primaire + secondaire	59	21	11	8	1	
Secteur tertiaire	64	20	11	4	1	
Activité locale/régionale	70	19	7	3	1	
Suisse	62	19	13	6		
Hors Suisse	44	26	17	12	1	
CA < 1mio	77	15	5	2	1	
CA 1-10 mio	63	19	10	7	1	
CA 10 mio et +	35	33	22	10		
< 30 employés	70	16	9	4	1	
30-100 employés	49	29	14	7	1	
100 employés et +	33	31	23	13		

4.3 Est-ce que les investissements nécessaires pour réparer les dégâts de cette (ces) attaque(s) ont été importants ou non pour votre entreprise ?

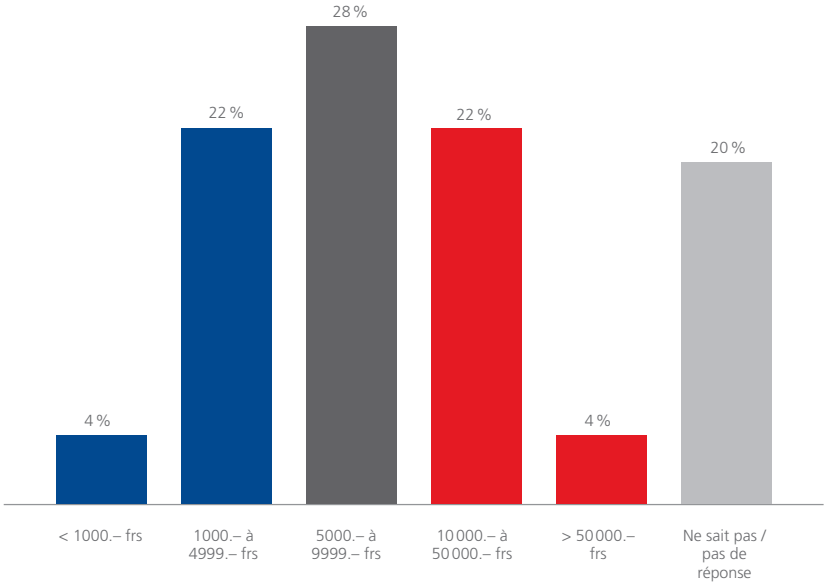
Base : 183 entreprises membres de la CVCI ayant subi au moins une attaque





4.4 Plus concrètement, combien vous ont coûté les investissements nécessaires pour réparer les dégâts de cette (ces) attaque(s) ?

Base : 50 entreprises membres CVCI avec investissements très / assez importants pour réparations



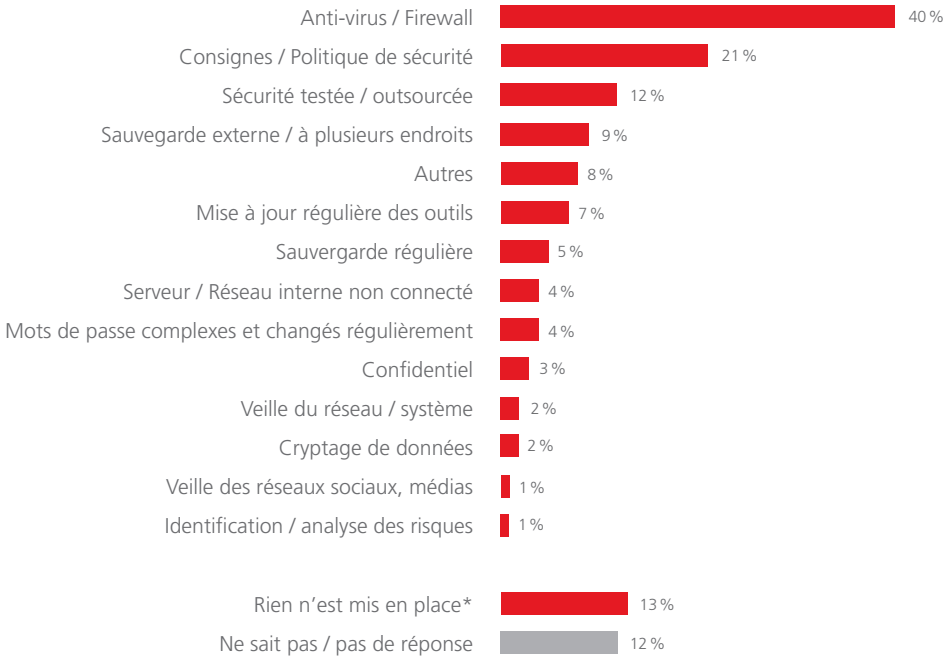
Au cas où l'absence de sauvegardes ou de procédures de récupération impose la reconstruction de tout le système informatique, la facture peut atteindre des dizaines de milliers de francs, estime l'expert Patrick Zwahlen. Dans notre enquête, deux entreprises reconnaissent des dommages d'une telle ampleur.

5. LES MESURES DE PROTECTION

5.1 Avez-vous mis en place des mesures de protection contre les cyber-risques dans votre entreprise ?

Base : 490 entreprises membres de la CVCI

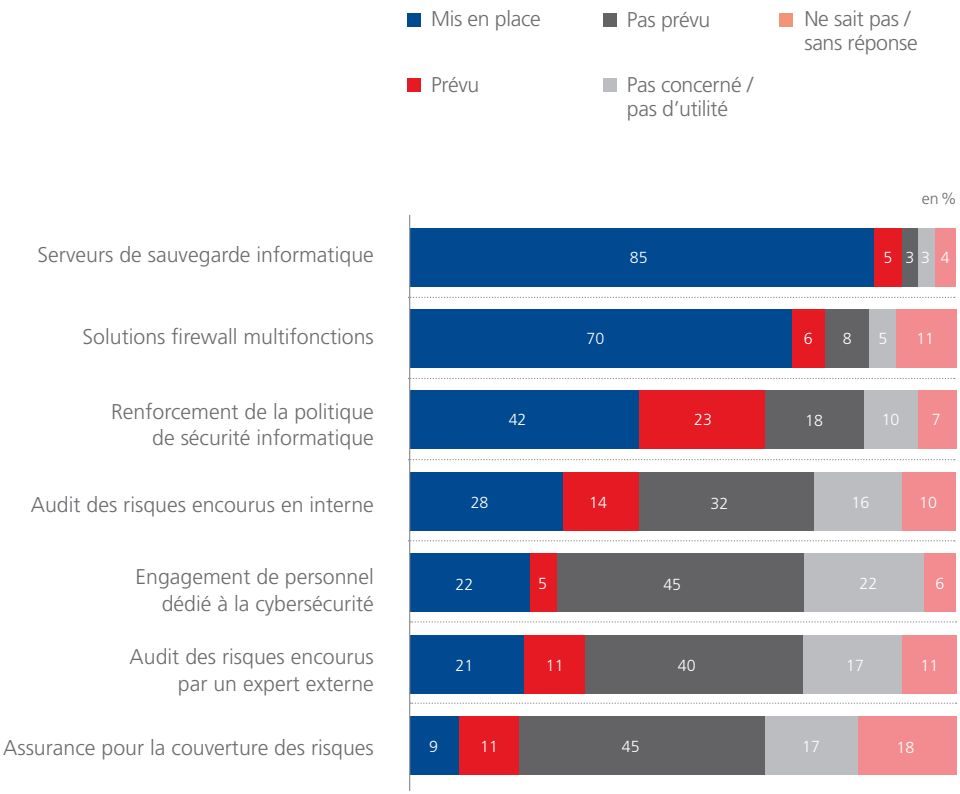
Réponses spontanées



* *Activité locale / régionale : 17 %*
CA < 1 mio : 23 %
< 30 employés : 16 %
Pas d'attaque / sans réponse : 15 %

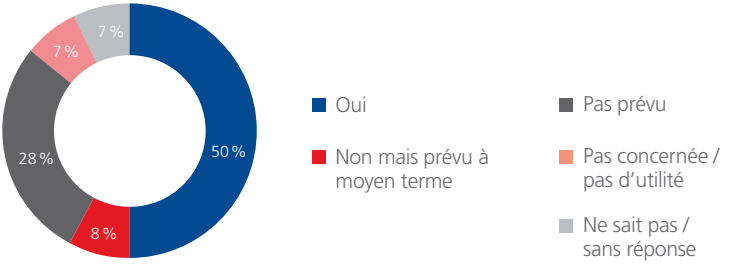
5.2 Voici quelques moyens pour se protéger de cyberattaques : pour chacun, veuillez indiquer si votre entreprise a déjà mis en place quelque chose de similaire, si ce sera fait à moyen terme ou si rien de tel n'est prévu actuellement.

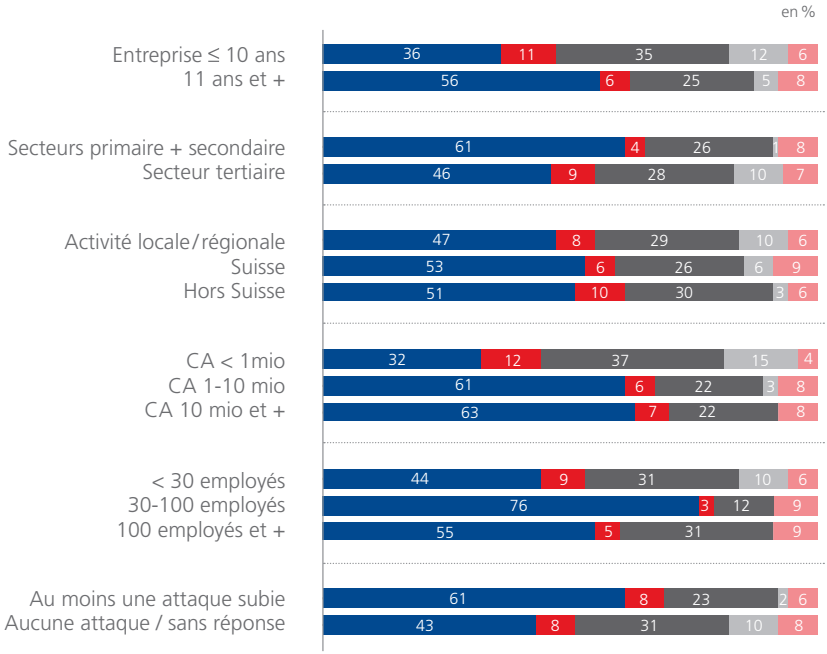
Base : 490 entreprises membres de la CVCI



5.3 Faites-vous appel à des entreprises spécialisées pour assurer la protection informatique de votre entreprise ?

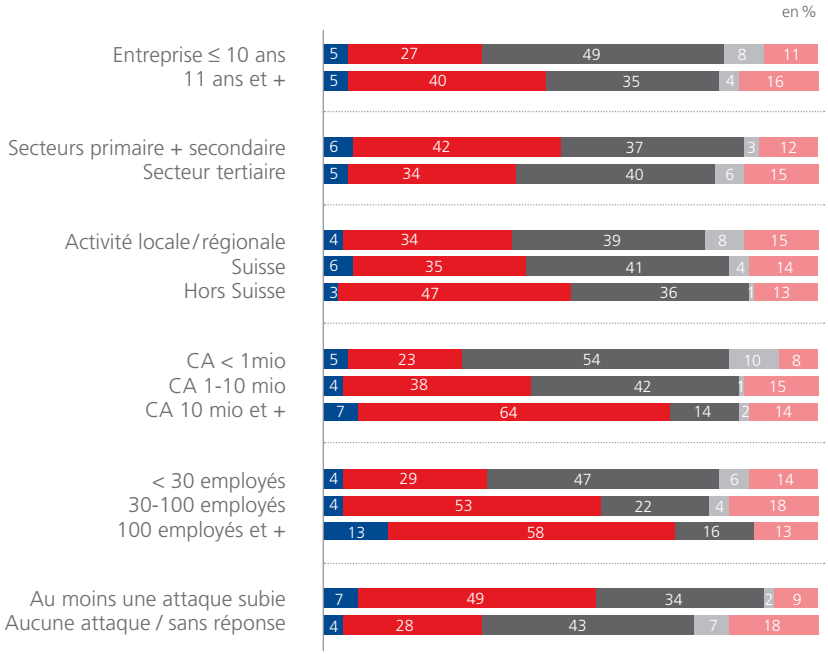
Base : 490 entreprises membres de la CVCI





5.4 La mise en place des diverses mesures pour se protéger de cyberattaques implique-t-elle des investissements importants ou non pour votre entreprise ?

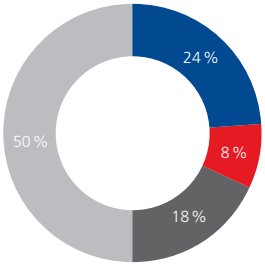
Base : 490 entreprises membres de la CVCI



6. LA PLACE DE LA FORMATION

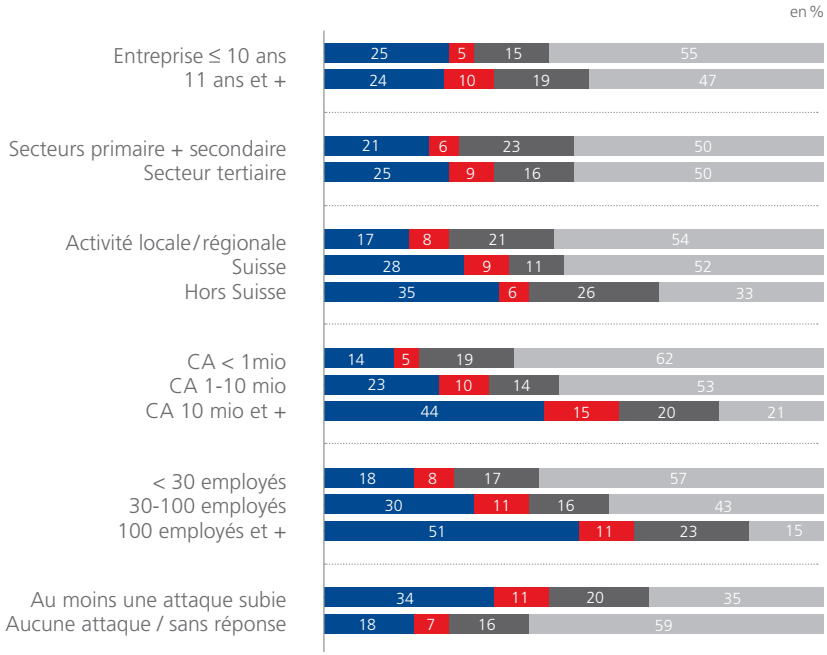
6.1 Est-ce que votre entreprise a mis en place des formations spécifiques (en interne ou auprès de tiers) en lien avec la cybersécurité ?

Base : 490 entreprises membres de la CVCI



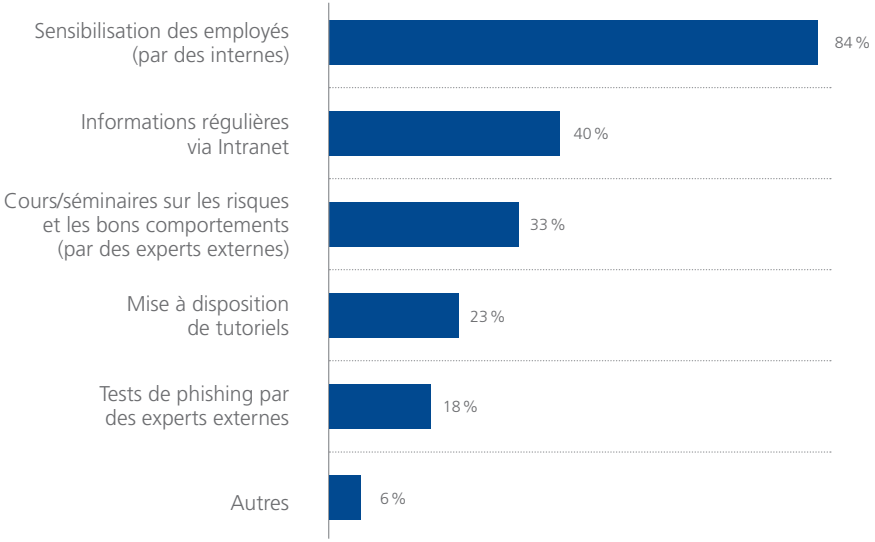
- Formations en cours / déjà faites
- En cours de réflexion
- Formations prévues
- Pas prévues / ne sait pas

Pour quels collaborateurs ? (B:245)
Tous les employés (78 %)
Direction (31 %)
Cadres supérieurs (24 %)
Cadres (20 %)
Autres employés (8 %)



6.2 En quoi consistent ces formations ?

Base : 245 entreprises membres de la CVCI qui ont fait ou prévu des formations

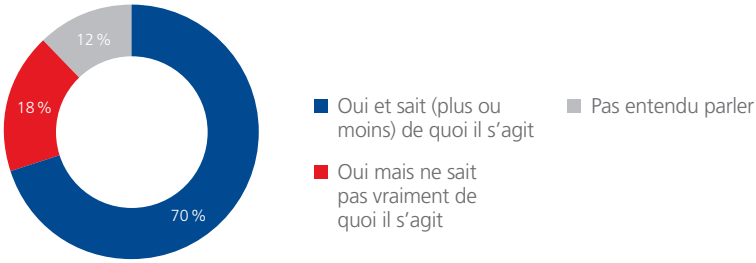


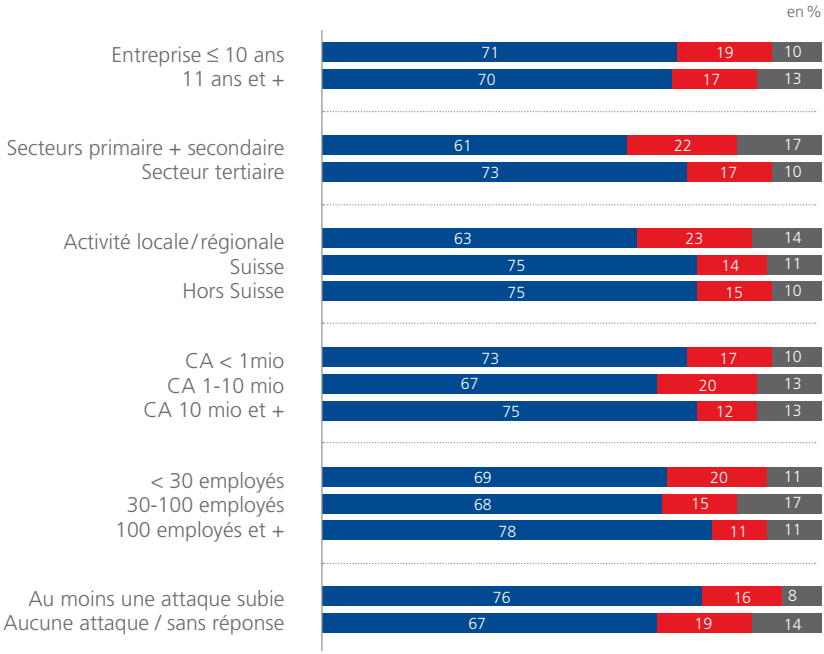
Idéalement, recommandent les experts consultés, il faudrait effectuer des tests de phishing deux ou trois fois par an dans chaque entreprise, compiler les statistiques et afficher les résultats en donnant des explications au personnel. On le voit, de tels tests ne sont guère répandus dans les entreprises vaudoises.

7. LA GESTION DES DONNÉES PERSONNELLES

7.1 Avez-vous entendu parler de l'entrée en vigueur du Règlement général européen sur la protection des données (RGPD), le 25 mai 2018 ?

Base : 490 entreprises membres de la CVCI

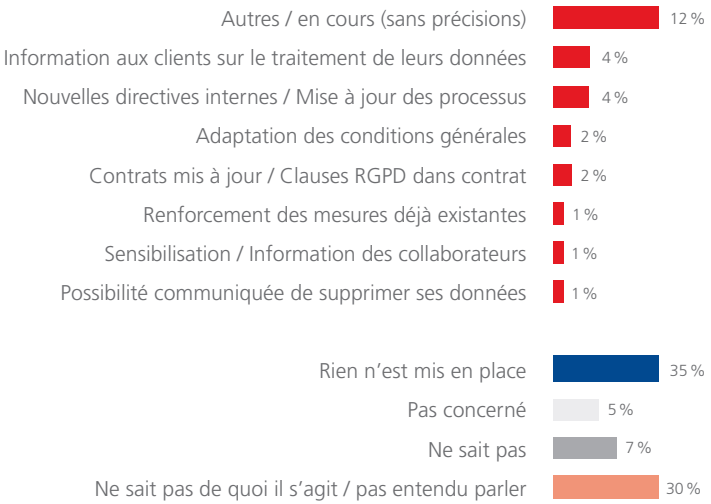




7.2 Avez-vous mis concrètement en place une nouvelle politique de gestion des données personnelles (de vos clients par exemple) pour vous mettre en conformité avec le Règlement général européen sur la protection des données (RGPD) ? Si oui, en quoi consiste-t-elle (ou consistera-t-elle) ?

Base : 490 entreprises membres de la CVCI

Réponses spontanées



Pour l'expert Eduardo Geraldi de CISEL Informatique SA, « l'entrée en vigueur du RGPD a permis de mettre la problématique au goût du jour, même si le sujet reste compliqué. L'Union européenne a fait un bon travail sur la protection des données, la gouvernance, ce qui a contribué à une prise de conscience à une échelle plus large. »

LES CLÉS DE LA SÉCURITÉ NUMÉRIQUE

« On le dit souvent, la question n'est pas de savoir si une entreprise va subir une cyberattaque, mais quand… Et c'est absolument vrai. » Cet avertissement, c'est l'expert Patrick Zwahlen, de Navixia, qui le lance avec gravité. Pour lui, toutes les entreprises, quelle que soit leur taille, sont susceptibles de voir leur système informatique victime d'une intrusion malveillante. Elles gèrent toutes de l'argent, et sont donc toutes intéressantes pour des hackers. Autant dire que le tiers des entreprises qui, selon notre enquête, estiment qu'elles ne sont pas concernées par les cyber-risques sous-estiment un danger auquel elles seront, tôt ou tard, confrontées.

Être en alerte doit devenir un réflexe !

Si elles se multiplient, ces attaques ne déploient pas toutes seules leurs conséquences funestes. Pour créer un dommage, il faut que quelqu'un clique sur une pièce jointe infectée ou sur un lien frauduleux. D'où l'importance d'informer le personnel sur les gestes à faire ou à ne pas faire. Les résultats du sondage réalisé par l'institut M.I.S Trend, sur mandat de la CVCI, montrent que si elle est un domaine globalement connu du monde de l'entreprise, la cybersécurité n'est pas toujours considérée avec suffisamment de rigueur. « Globalement, estime Patrick Zwahlen, le sentiment de sécurité prévalant dans notre pays incite peut-être les entreprises, notamment leurs dirigeants seniors, à sous-estimer les risques. Mais dans le monde digitalisé d'aujourd'hui, cette attitude confine à l'insouciance. On voit que les entreprises qui travaillent à l'international sont clairement plus sensibles à la problématique que celles qui ont des activités uniquement en Suisse. »

Sous-estimation des risques, sous-équipement matériel, carences en termes de sensibilisation et de formation: les manquements sont réels et appellent une prise en considération rapide et déterminée de cette problématique vitale pour la pérennité des entreprises. État des lieux et esquisse de solutions en six points.

1. DIVERSES MANIÈRES DE S'INFORMER

À l'heure actuelle, il est difficile de passer à côté de la thématique cybersécuritaire, extrêmement présente dans les médias. Notre enquête indique que 73 % des entrepreneurs s'informent sur le sujet, et un quart pas particulièrement. Ce dernier chiffre interpelle et montre qu'une partie d'entre eux sous-estime ces dangers, tant il est vrai que les cybercriminels sont à l'œuvre sans relâche. Parmi les trois-quarts de sondés qui disent s'informer de manière générale sur le sujet, 77 % le font à travers les médias, 70 % via Internet, 45 % par le bouche à oreille. Un tiers seulement par le biais des autorités et/ou à travers des formations. Cette dernière proportion donne deux indications claires: il existe un manque d'informations émanant des autorités et les entreprises recourent insuffisamment à la sensibilisation et à la formation. Cela dit, comme le souligne l'expert Patrick Zwahlen, « il peut y avoir un ‹effet *20 minutes*›: un article sur des attaques informatiques peut provoquer une prise de conscience. »

2. SENSIBILISER ET FORMER

Les spécialistes de la cybersécurité le clament à l'unisson : le meilleur moyen de parer une attaque informatique consiste à sensibiliser les collaborateurs, dans un premier temps, puis à les former. Être en alerte doit devenir un réflexe ! Une entreprise aura beau disposer des meilleurs systèmes de protection, elle ne pourra rien face à la méconnaissance ou à la négligence du personnel qui est, dans l'immense majorité des cas, la cause d'une intrusion funeste dans les systèmes informatiques. Par son comportement, un collaborateur peut mettre en danger l'entreprise pour laquelle il travaille, et pas uniquement en cliquant malencontreusement sur une pièce jointe malicieuse. Il existe aussi un lien entre les cyber-risques au niveau du domicile et leur propagation au sein de l'entreprise.

En cause: les périphériques nomades (laptops, clés USB, smartphones, etc.). Ce nomadisme peut faire rentrer des malwares, des chevaux de Troie ou autres virus dans l'espace professionnel. « Beaucoup d'entrepreneurs partent du principe que les gens savent, alors qu'ils ne savent pas! Il existe donc un grand besoin de formation », assure Stéphane Koch, expert en sécurité de l'information, et vice-président d'High-Tech Bridge. « Seules la sensibilisation et la formation permettent de lutter efficacement contre ces attaques, estime Patrick Zwahlen. Une bonne hygiène informatique est bénéfique aussi bien au travail qu'à la maison. »

Cela dit, on parle de sensibiliser, mais de quelle manière ? Qui prend l'initiative et la responsabilité de faire les choses ? Au sein des grandes entreprises, le conseil d'administration est responsable de la mise en place d'une politique de sécurité numérique efficace. « Il faut une vraie prise de conscience à tous les niveaux de l'entreprise, assure Eduardo Geraldi, Head of ICT Consulting et CISO chez CISEL Informatique SA. S'agissant des grandes sociétés, il faut une personne experte de la cybersécurité au niveau du conseil d'administration. Dans les grandes structures, il y a un responsable sécurité au niveau opérationnel en général, mais pas au sein des petites entreprises. Les PME doivent trouver le bon partenaire. Il faut bien mesurer les risques, comme pour une voiture : casco totale ou partielle ? ».

Il faut intégrer peu à peu les employés dans la dynamique de sécurité.

Notre enquête révèle que seul un tiers des entreprises sondées ont mis en place des formations, ou sont sur le point de le faire. Les petites entreprises, en particulier, ont des carences dans ce domaine. Un peu moins de 20 % y réfléchissent alors que 50 % n'y songent pas ! Parmi celles qui en proposent, 84 % privilégient la sensibilisation des employés à l'interne, 40 % prodiguent des infos régulières via Intranet et un tiers offrent des cours sur les risques par le biais d'experts externes. Une analyse fine des données de notre enquête montre que les cadres manquent de temps pour se former, alors qu'ils sont des cibles privilégiées des cybercriminels. Et qu'ils représentent donc un risque plus important.

Idéalement, recommandent les experts consultés, il faudrait effectuer des tests de phishing deux ou trois fois par an dans chaque entreprise, compiler les statistiques et afficher les résultats en donnant des explications au personnel. L'idée ? Montrer que cela s'améliore, féliciter les collaborateurs, et encourager les bons comportements en remettant, par exemple, un prix. La notion de « charte » peut également être intéressante. Il s'agit d'expliquer aux gens la bonne utilisation de l'outil informatique, souvent complexe. L'entreprise est aussi responsable de dire aux collaborateurs ce qu'ils peuvent faire ou non. Cette charte pourrait figurer en annexe au contrat de travail. Des politiques de sécurité devraient être mises en place. Pour Stéphane Koch, les entreprises peuvent proposer une formation de base, puis profiter des Intranet pour la faire évoluer avec, par exemple, une explication pédagogique de cas d'attaques dont ont été victimes d'autres entreprises, et les bons comportements à adopter, ou des quiz comme forme de piqûres de rappel. Il faut intégrer peu à peu les employés dans la dynamique de sécurité : ils peuvent être une menace pour la sécurité de l'entreprise, mais aussi garants de celle-ci s'ils sont bien formés et ainsi, également, de leur emploi. A l'ère des médias sociaux, ils sont aussi constitutifs de la réputation de l'entreprise.

3. PROTÉGER, STOCKER ET ÊTRE PRÊT À RÉPARER

À côté de la sensibilisation et la formation du personnel, il est évidemment indispensable de disposer d'un matériel performant et mis à jour. Cela implique des coûts que toutes les PME ne peuvent s'offrir, ce d'autant plus que les patrons de petites entreprises ne voient pas de retour

sur investissement direct. « Cela dit, c'est un peu comme l'assurance-maladie: elle coûte cher jusqu'à ce que l'on tombe malade », insiste Stéphane Koch. Notre enquête montre que la grande majorité des sondés a conscience de la nécessité de prendre des mesures de protection (serveurs de sauvegarde, antivirus et pare-feu, politiques de sécurité, etc.). Mais peu ont fait procéder à des audits de sécurité. 41 % des sondés (en moyenne) estiment que la mise en place de mesures pour se protéger représente des investissements très importants à assez importants. Ce chiffre est bien plus élevé dans les grandes et moyennes entreprises.

Autre chiffre saillant de notre enquête : 50 % des répondants disent externaliser leur protection informatique. C'est une solution. « Malheureusement, on se trouve face à un manque de personnel qualifié dans le domaine de la sécurité en Suisse », observe Patrick Zwahlen. La quantité de ressources est insuffisante. Pour le reste, rappelons que la sécurité des données relève de la responsabilité des entreprises, et qu'elles ne peuvent pas s'en exonérer en externalisant.

Le stockage est un point central de la sécurité informatique. Il convient de réfléchir au type de données dont on dispose et au lieu où on les héberge. Près de 90 % des entreprises sondées ont mis en place des serveurs de sauvegarde. C'est bien. Mais encore faut-il savoir comment et où… Selon Stéphane Koch, l'idéal est de stocker les données sur plusieurs périphériques distincts et d'avoir deux lieux de stockage et trois versions séparées de son système et/ou de ses fichiers, à savoir dans l'entreprise et à l'extérieur, car il peut y avoir des dégâts d'eau, un incendie, des vols de données. Ces sauvegardes doivent être faites alternativement entre un support et un autre... Et pas seulement les backups des données, mais aussi les images du système d'exploitation à un moment donné (Snapshot), de sorte qu'on n'ait pas à réinstaller tous les programmes et à tout reconfigurer. Pour lui, les données devraient être chiffrées sur tout support, sous clé. Et sans verser dans la paranoïa, il rappelle la nécessité de faire des vérifications régulières et aléatoires des sauvegardes. Et le cloud ? C'est un très bon complément à un backup sur un support physique, mais il faut veiller selon lui à l'aspect juridique, avec qui l'on travaille. Si un prestataire cloud à l'étranger fait faillite, on ne peut guère espérer récupérer quoi que ce soit et être dédommagé. Il vaut mieux sauvegarder en Suisse, estime l'expert, car il sera potentiellement plus facile d'obtenir réparation le cas échéant.

Près de 90 % des entreprises sondées ont mis en place des serveurs de sauvegarde. C'est bien. Mais encore faut-il savoir comment et où…

Malgré toutes les précautions prises, une attaque peut survenir et, hélas, causer des dommages. Un tiers des entreprises que nous avons sondées disent avoir subi au moins une cyberattaque. Un gros quart d'entre elles concèdent avoir dû investir des sommes conséquentes pour réparer les dégâts : 22 % de celles-ci ont dû débourser entre 10 000 et 50 000 francs, alors que pour 4 %, la facture a excédé les 50 000 francs. On le voit, ces sommes peuvent être très élevées. Si gouverner c'est prévoir, réparer c'est anticiper. Il faut, en amont, avoir prévu des procédures. Selon Patrick Zwahlen, lorsqu'une attaque impose de restaurer des backup et de reconstruire des serveurs, le coût d'une telle opération peut osciller entre 2000 et 5000 francs pour les cas les plus courants. En revanche, au cas où l'absence de sauvegardes ou de procédures de récupération impose la reconstruction de tout le système informatique, la facture peut atteindre des dizaines de milliers de francs. Pour l'entreprise, il est donc très important d'anticiper les risques, de s'assurer que les sauvegardes sont régulières et récupérables, et de prévoir un plan d'action en cas d'attaque. Elle peut ainsi limiter les risques, contenir efficacement les situations critiques et s'économiser beaucoup de soucis, de temps et d'argent.

4. L'IMPORTANCE DES DONNÉES PERSONNELLES

Notre enquête portait également sur la gestion des données personnelles, à la lumière de l'entrée en vigueur du Règlement général européen sur la protection des données (RGPD), le 25 mai 2018. Il concerne la Suisse même si celle-ci ne fait pas partie de l'Union européenne (UE). La CVCI a organisé des séminaires sur la question à l'intention de ses membres, a produit des vidéos et des fiches juridiques. Cette nouvelle réglementation a été largement médiatisée, au point qu'il est difficile de ne pas en avoir entendu parler. Cependant, notre enquête indique que 30 % des entreprises sondées ne savent pas vraiment de quoi il s'agit ou ignorent de quoi il retourne. Un chiffre qui a étonné nos experts, mais qui n'a pu que diminuer depuis l'été.

Même si une grande partie du RGPD est déjà contenue dans la Loi suisse sur la protection des données, dont la révision traîne aux Chambres fédérales, les entreprises ne semblaient pas vraiment conscientes de leur responsabilité par rapport aux informations personnelles en leur possession jusqu'à présent. Le règlement européen va les obliger à en faire l'inventaire, à établir des référentiels à l'interne et à réfléchir auxquelles tombent sous le coup de cette réglementation. Pour l'expert Eduardo Geraldi, « l'entrée en vigueur du RGPD a permis de mettre la problématique au goût du jour, même si le sujet reste compliqué. L'Union européenne a fait un bon travail sur la protection des données, la gouvernance, ce qui a contribué à une prise de conscience à une échelle plus large. »

5. LE RÔLE DES COLLECTIVITÉS PUBLIQUES

En Suisse, on ne dispose hélas que de peu de données mettant en évidence l'ampleur des dommages causés par la cybercriminalité, alors qu'en France, on lui attribue entre 6 et 8 milliards d'euros de pertes pour l'économie en 2017. Pour Stéphane Koch, de tels indicateurs devraient être disponibles au niveau du Secrétariat d'État à l'économie (SECO). « Ce n'est pas de l'informatique, mais de l'économie. Sécuriser nos données constitue une manière de préserver la matière première que représentent nos entreprises ! » relève-t-il encore.

En Suisse, on ne dispose hélas que de peu de données mettant en évidence l'ampleur des dommages causés par la cybercriminalité.

Les choses bougent toutefois à l'échelon fédéral. Après bien des tergiversations, les sept Sages ont décidé d'intensifier leurs efforts en matière de prévention et de lutte contre les cyber-risques. En juillet dernier, le Conseil fédéral a pris les premières décisions de principe et attribué différents mandats en vue de la création d'un centre de compétence dans ce domaine. Les contours du projet définitif sont attendus pour la fin de cette année. De son côté, l'Office fédéral pour l'approvisionnement économique du pays (OFAE) a mené une réflexion sur la vulnérabilité aux risques numériques dans divers domaines vitaux de l'économie suisse, comme l'approvisionnement en électricité, en eau potable et en aliments, ainsi que les transports par la route et le rail. Fort de ces résultats, l'Office a mis au point une norme minimale pour les Technologies de l'information et de la communication (TIC) afin d'améliorer la résilience informatique, plus spécialement destinée aux exploitants d'infrastructures critiques en Suisse, mais toute entreprise peut l'appliquer. Cette norme comprend diverses fonctions: identifier, protéger, détecter, réagir et récupérer. Elle donne aux utilisateurs 106 indications concrètes pour améliorer la résilience de leurs systèmes d'information face aux cyber-risques. « C'est une très bonne chose qu'on puisse donner aux entreprises cet outil, qui est inspiré du NIST Framework américain, estime l'expert Eduardo Geraldi. Les PME peuvent appliquer ces mesures et faire évoluer leur ‹hygiène informatique›. »

Autre initiative à saluer: un groupe d'experts privé-public a lancé, au début du mois de septembre,

un test rapide disponible sur le Web, qui doit permettre aux PME de vérifier en vingt minutes si elles sont suffisamment protégées face aux pirates informatiques et autres dangers de la Toile.

Le canton de Vaud tire son épingle du jeu. La Police cantonale lance régulièrement des campagnes de sensibilisation sur les cyber-risques à l'intention des entreprises, en collant au plus près à l'actualité selon les types d'attaques en cours. Elle a publié, en novembre 2017, un numéro hors-série de son magazine *Polcant info* consacré notamment à la prévention et à la sécurité en entreprise. Consciente que le phénomène des cyberattaques va aller en s'amplifiant, la police vaudoise va publier sous peu une série d'articles à propos de ce thème sur le site votrepolice.ch. Elle vient en outre de lancer une campagne de prévention concernant les cyber-risques sur sa page LinkedIn, à l'intention du monde de l'économie. Le canton a fait de la cybersécurité une priorité. Main dans la main, la Police cantonale, le centre de compétences de cybersécurité de la Direction des systèmes d'information (DSI) et la promotion économique avec Innovaud ont mis au point une application à l'intention des entreprises vaudoises. Celle-ci développe en particulier un set de dix bonnes pratiques qui, si elles sont suivies, permettent de réduire les risques contre les actions des criminels du Web et d'y répondre, le cas échéant, d'une manière adéquate. « Il s'agit essentiellement de mesures simples qui permettent de construire un rempart efficace contre les cyberattaques », explique Marc Barbezat, responsable Sécurité IT et Cybersécurité à la DSI. On trouvera aussi sur cette application une liste de sociétés vaudoises spécialisées dans la cybersécurité auxquelles les entrepreneurs pourront recourir. Il est également prévu de diffuser des alertes pour les PME en cas, par exemple, de menaces ciblant le canton de Vaud. Sa sortie est imminente.

6. DES COMPÉTENCES À VALORISER

La Suisse, et le canton de Vaud en particulier, regorge de compétences dans les domaines de la sécurité au sens large et de la cybersécurité. Autour de Lausanne et d'Yverdon-les-Bains, la concentration d'entreprises spécialisées dans la sécurité informatique (notamment SCRT, Kudelski Security, Vigiswiss), de centres de recherche et d'incubateurs de haut niveau, démontre la formidable effervescence créatrice qui règne dans l'ensemble des secteurs concernés par ce domaine. L'émergence, en décembre dernier, d'un Center for digital trust (Centre pour la confiance numérique) à l'École polytechnique fédérale de Lausanne (EPFL), illustre ce foisonnement. Cette plateforme ambitionne de devenir un pôle de référence numérique dans les domaines de la sécurité informatique, de la protection des données et du respect de la vie privée. La Haute école pourra compter sur le soutien de partenaires industriels et institutionnels. La HEIG-VD possède pour sa part un pôle de compétences en sécurité informatique formé d'une douzaine de spécialistes. Ses activités de R&D ont permis le développement de plusieurs start-up, dont NetGuardians, StrongCodes et Sysmosoft.

En clair, la convergence de ces multiples compétences et initiatives publiques et privées apporte non seulement une grande visibilité nationale et internationale au canton de Vaud, à l'Arc lémanique et à la Suisse dans le domaine des technologies de la confiance et de la sécurité, mais pose également les jalons d'une nouvelle « TrustTech Valley ».

CONCLUSION

C'est un fait acquis : l'interconnexion croissante des infrastructures, processus et données des entreprises à Internet accroît de manière substantielle les risques liés au cyberespace. Notre enquête montre que les PME n'ont, de loin, pas toutes

conscience de ces dangers et de leurs conséquences. Elles doivent impérativement prendre en compte ce paramètre dans leur réflexion stratégique et mettre en place des dispositifs de défense adaptés, en élaborant notamment des plans d'urgence. Surtout, et c'est là que se situe le fondement de l'édifice sécuritaire à bâtir, elles doivent sensibiliser très régulièrement leurs collaborateurs dans ce domaine.

S'équiper de matériel fiable, procéder à un audit de sécurité, former le personnel et effectuer des tests réguliers ne coûte pas une fortune : cela devrait même relever de l'investissement de base pour toute entreprise. Car réparer les dommages causés par une cyberattaque peut induire des coûts autrement plus élevés, sans parler des dégâts d'image. Espérer passer entre les gouttes est illusoire à en croire les experts que nous avons consultés pour cette enquête.

La CVCI s'engage pour informer ses membres sur les risques liés à la criminalité informatique. Elle a ainsi mis sur pied nombre d'événements sur cette thématique, dont le dernier en date, le 25 septembre, avait pour thème « La cybersécurité, la priorité stratégique des dirigeants », en partenariat avec CISEL Informatique SA et Insurance Broking and Consulting SA. Et elle va poursuivre ses efforts dans ce domaine. Les petites et moyennes entreprises constituent la colonne vertébrale de l'économie vaudoise. Garantes de la prospérité du canton, elles doivent se préserver au mieux du péril cyberspatial.

Différents acteurs (canton, police) ont eux aussi compris ces enjeux et se mobilisent. D'autres défis de taille se profilent à brève échéance : il s'agira de former davantage de spécialistes et d'encourager des entreprises spécialisées dans le domaine à naître en Suisse, afin de répondre à une demande grandissante que le marché actuel peine à couvrir.

LES BONS RÉFLEXES CYBERSÉCURITAIRES

1. Définir un responsable cybersécurité (au besoin, un expert externe)
2. Faire réaliser un audit de sécurité
3. S'équiper de matériel fiable mis à jour régulièrement
4. Sensibiliser et former le personnel de l'entreprise
5. Procéder à des sauvegardes de données périodiques (backup)
6. Effectuer des tests de phishing réguliers

* Sur la plateforme vaud.digital, vous pouvez retrouver une liste des entreprises vaudoises spécialisées dans la cybersécurité, à l'adresse précise https://bit.ly/2NaHoyJ ou via le QR code.

CHAMBRE VAUDOISE DU COMMERCE ET DE L'INDUSTRIE
Avenue d'Ouchy 47
1006 Lausanne

TÉLÉPHONE + 41 (0)21 613 35 35
FAX + 41 (0)21 613 35 05

E-MAIL cvci@cvci.ch
WEB www.cvci.ch

TRANSPORTS PUBLICS
M2 ou bus TL n° 2 Maladière-Désert : arrêts Jordils

HORAIRES D'OUVERTURE
Lundi au vendredi
07 h 45 – 12 h 00
13 h 30 – 17 h 00